Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method for performing data integration between two or more computer systems provided over a network, the method comprising:

extracting data from a first volume of a storage system, the first volume associated with a first computer system of first type, the extracted data having a first file format and a first character-set format, the storage system being coupled to a plurality of computer systems;

encrypting the data using a first security key;

storing the encrypted data **and a signature file** in a shared volume of the storage system;

receiving the encrypted data **and the signature file** from the shared volume of the storage system at a second computer system of second type, the first and second computer system being of different computer systems, wherein the second computer system comprises a file receiver, a file format converter, a data decryptor, a character set converter, a database loader, a signature receiver, and a signature checker;

converting the ~~received data~~ **encrypted data and the signature file** from the first file format to a second file format with the file format converter, the first file format being native to the first computer system and the second file format being native to the second computer system;

determining whether the signature file is authenticated by the first security key;

if the signature file is authenticated, decrypting the ~~received data~~ **encrypted** data using a second security key that is associated with the first security key;

converting the ~~received~~**decrypted** data from the first character-set format to a second character-set format with the character set converter, the first character-set format being native to the first computer system, the second character-set format being native to the second computer system; and

thereafter, loading the ~~received~~**decrypted** data with the database loader to a second volume of the storage system, the second volume associated with the second computer system.

2. (Original) The method of claim 1, wherein the first computer system is a mainframe system, and the second computer system is an open system, and the plurality of computer systems being associated with a plurality of different companies.

3. (Previously Presented) The method of claim 1, wherein the first file format is a count key data format.

4. (Original) The method of claim 3, wherein the second file format is a fixed block architecture format.

5. (Original) The method of claim 1, wherein the first character-set format is an Extended Binary Coded Decimal Interchange Code (EBCDIC) format.

6. (Original) The method of claim 1, wherein the second character-set format is an American Standard Code for Information Interchange(ASCII) format.

7. (Original) The method of claim 1, wherein the first security key is a public key associated with the second computer system, and the second security key is a private key associated with the second computer system.

8. (Original) The method of claim 1, wherein the first security key is a private key associated with the first computer system, and the second security key is a public key associated with the first computer system.

9. (Original) The method of claim 1, wherein the first and second computer systems are coupled to the storage system via a storage area network and the storage system includes at least one disk array unit, wherein the first security key and the second security key are common keys.

10. (Previously Presented) The method of claim 1, further comprising:

storing the encrypted data in a third volume of the storage system, the third volume being associated with the first computer system,

wherein the plurality of computer systems are associated with a plurality of different companies.

11. (Original) The method of claim 10, wherein the shared volume is configured to be accessed only by computer systems of a given company, the first and second computer systems being associated with the given company.

12. (Original) The method of claim 1, wherein the step of decrypting the received data using a second security key is performed after the step of converting the received data from the first file format to a second file format, and the step of converting the received data from the first character-set format to a second character-set format is performed after the step of decrypting the received data using a second security key.

13. (Original) The method of claim 1, further comprising:

generating a digital signature of the first computer system using the extracted data;

transmitting the digital signature from the first computer system to the second computer system;

receiving the digital signature at the second computer system; and

validating the received digital signature at the second computer system.

14. (Original) The method of claim 13, wherein the digital signature is transmitted from the first computer system to the second computer system via a first communication link that is different from a second communication link that is used to transfer the data from the first computer system to the second computer system.

15. (Canceled)

16. (Currently amended) A method for sharing data between a plurality of computer systems sharing a storage system, the method comprising:

receiving **[[an]]** encrypted data **and a signature file** from a shared volume of the storage system at a second computer system of second type, the encrypted data being data that has been extracted from a first volume of the storage system that is associated with a first computer system of first type, the received data having a first format and a third format, wherein the second computer system comprises a file receiver, a file format converter, a data decryptor, a character set converter, a database loader, a signature receiver, and a signature checker;

converting the ~~received data~~ **encrypted data and the signature file** from the first format to a second format with the file format converter, the first format being native to the first computer system and the second format being native to the second computer system;

determining whether the signature file is authenticated by the first security key;

if the signature file is authenticated, decrypting with the data decryptor the ~~received~~ **encrypted** data using a second security key that is associated with a first security key that has been used to encrypt the extracted data at the first computer system; and

thereafter, loading with the data loader the **decrypted** data to a second volume of the storage system, the second volume being associated with the second computer system.

17. (Previously Presented) The method of claim 16, further comprising:

converting the received data from the third format to a fourth format, the third format being native to the first computer system, the fourth format being native to the second computer system.

18. (Original) The method of claim 17, wherein the first format is a file format of first type, and the second format is a file format of second type.

19. (Original) The method of claim 17, wherein the third format is a character-set of first type, and the fourth format is a character-set of second type.

20. (Previously Presented) The method of claim 19, wherein the step of converting the received data from the third format to a fourth format is performed after the step of decrypting the received data using a second security key, and the step of decrypting the received data using a second security key is performed after the step of converting the received data from the first format to a second format.

21. (Original) The method of claim 16, further comprising:

receiving a digital signature of the first computer, the digital signature being associated with the received data; and

authenticating the digital signature of the first computer system.

22. (Original) The method of claim 21, wherein the digital signature is received via a local area network and the data is received via a storage area network.

23. – 25. (Canceled)